Esempio di configurazione di Usa mapping di attributi LDAP

Sommario

Introduzione

In questo documento viene descritto come mappare qualsiasi attributo Microsoft/AD a un attributo Cisco.

Procedura

1. Sul server Active Directory (AD)/Lightweight Directory Access Protocol (LDAP):Scegliere **utente1**.Fate clic con il pulsante destro del mouse su **> Proprietà (Properties)**.Scegliere una scheda da utilizzare per impostare un attributo, ad esempio la scheda Generale.Scegliere un campo o un attributo, ad esempio il campo Office, da utilizzare per applicare l'intervallo di tempo, quindi immettere il testo dell'intestazione (ad esempio, Benvenuto in LDAP !!!). La configurazione di Office nella GUI è memorizzata nell'attributo physicalDeliveryOfficeName di AD/LDAP.
2. Per creare una tabella di mapping degli attributi LDAP sull'appliance ASA (Adaptive Security Appliance), mappare l'attributo PHYSICALDeliveryOfficeName di AD/LDAP all'attributo ASA Banner1:

```
B200-54(config)# show run ldap
ldap attribute-map Banner
map-name physicalDeliveryOfficeName Banner1
```

3. Associare la mappa degli attributi LDAP alla voce aaa-server:

```
B200-54(config-time-range)# show runn aaa-server microsoft
aaa-server microsoft protocol ldap
aaa-server microsoft host audi-qa.frdevtestad.local
ldap-base-dn dc=frdevtestad,dc=local
ldap-scope subtree
ldap-naming-attribute sAMAccountName
ldap-login-password hello
ldap-login-dn cn=Administrator,cn=Users,dc=frdevtestad,dc=local
ldap-attribute-map Banner
```

4. Stabilire la sessione di Accesso remoto e verificare che all'utente VPN venga visualizzato il messaggio di benvenuto del banner in LDAP !!!.

Inserire utenti LDAP in un oggetto Criteri di gruppo specifico (esempio generico)

In questo esempio viene illustrata l'autenticazione di user1 sul server AD-LDAP e viene recuperato il valore del campo Department in modo che possa essere mappato a un criterio di gruppo ASA/PIX da cui è possibile applicare i criteri.

1. Sul server AD/LDAP:Scegliere **utente1**.Fate clic con il pulsante destro del mouse su **> Proprietà (Properties)**.Scegliere una scheda da utilizzare per impostare un attributo, ad esempio la scheda Organizzazione.Scegliere un campo o un attributo, ad esempio Reparto, da utilizzare per applicare un criterio di gruppo e immettere il valore del criterio di gruppo (Criteri di gruppo 1) sull'appliance ASA/PIX. La configurazione Department (Reparto) sulla GUI è memorizzata nel reparto AD/LDAP (attributo).
2. Definire una tabella ldap-attribute-map.

```
5520-1(config)# show runn ldap
ldap attribute-map Our-AD-Map
map-name department Group-Policy
5520-1(config)#
```

3. Definire i criteri di gruppo Criteri_gruppo1 sull'accessorio e gli attributi dei criteri richiesti.
4. Stabilire il tunnel di accesso remoto VPN e verificare che la sessione erediti gli attributi da Criteri di gruppo 1 e gli altri attributi applicabili dai Criteri di gruppo predefiniti. **Nota**: aggiungere altri attributi alla mappa in base alle esigenze. In questo esempio viene mostrato solo il minimo per controllare questa funzione specifica (posizionare un utente in una specifica ASA/PIX 7.1.x). Nel terzo esempio viene illustrato questo tipo di mappa.

Configurare un criterio di gruppo NOACCESS

Èpossibile creare un criterio di gruppo NOACCESS per negare la connessione VPN quando l'utente non fa parte di alcun gruppo LDAP. Di seguito è riportato il frammento di configurazione da utilizzare come riferimento:

```
group-policy NOACCESS internal
group-policy NOACCESS attributes
vpn-simultaneous-logins 0
vpn-tunnel-protocol IPSec webvpn
```

Ènecessario applicare questo criterio di gruppo come criterio di gruppo predefinito al gruppo di tunnel. In questo modo, gli utenti che ottengono un mapping dalla mappa degli attributi LDAP, ad esempio gli utenti che appartengono a un gruppo LDAP desiderato, possono ottenere i criteri di gruppo desiderati e gli utenti che non ottengono alcun mapping, ad esempio gli utenti che non

appartengono a nessuno dei gruppi LDAP desiderati, possono ottenere i criteri di gruppo NOACCESS dal gruppo di tunnel, che ne blocca l'accesso.

> **Suggerimento**: poiché qui l'attributo vpn-simultous-logins è impostato su 0, deve essere definito esplicitamente anche in tutti gli altri criteri di gruppo. In caso contrario, può essere ereditato dal criterio di gruppo predefinito per quel gruppo di tunnel, che in questo caso è il criterio NOACCESS.

Applicazione dei criteri per gli attributi basati su gruppo (esempio)

1. Nel server AD-LDAP, Utenti e computer di Active Directory, impostare un record utente (VPNUserGroup) che rappresenta un gruppo in cui sono configurati gli attributi VPN.
2. Nel server AD-LDAP Utenti e computer di Active Directory definire il campo Reparto di ogni record utente in modo che punti al record gruppo (VPNUserGroup) nel passaggio 1. Il nome utente in questo esempio è web1. **Nota**: l'attributo Department AD è stato utilizzato solo perché reparto fa riferimento in modo logico al criterio di gruppo. In realtà, è possibile utilizzare qualsiasi campo. È necessario che questo campo sia mappato all'attributo VPN di Cisco Criteri di gruppo, come mostrato nell'esempio.
3. Definire una tabella ldap-attribute-map:

   ```
   5520-1(config)# show runn ldap
   ldap attribute-map Our-AD-Map
   map-name department IETF-Radius-Class
   map-name description\Banner1
   map-name physicalDeliveryOfficeName IETF-Radius-Session-Timeout
   5520-1(config)#
   ```

   I due attributi AD-LDAP Description e Office (rappresentati dai nomi AD description e PhysicalDeliveryOfficeName) sono gli attributi dei record del gruppo (per VPNUSerGroup) che vengono mappati agli attributi VPN di Cisco Banner1 e IETF-Radius-Session-Timeout.L'attributo department consente al record utente di eseguire il mapping al nome dei criteri di gruppo esterni sull'appliance ASA (VPNUSer), che quindi esegue il mapping al record VPNuserGroup sul server AD-LDAP, in cui sono definiti gli attributi.**Nota**: l'attributo Cisco (Criteri di gruppo) deve essere definito nella mappa degli attributi ldap. L'attributo AD mappato può essere qualsiasi attributo AD impostabile. In questo esempio viene utilizzato il nome reparto perché è il nome più logico che fa riferimento ai criteri di gruppo.
4. Configurare il server aaa con il nome della mappa attributi ldap da utilizzare per le operazioni di autenticazione LDAP, autorizzazione e accounting (AAA):

   ```
   5520-1(config)# show runn aaa-server LDAP-AD11
   aaa-server LDAP-AD11 protocol ldap
   aaa-server LDAP-AD11 host 10.148.1.11
   ldap-base-dn cn=Users,dc=nelson,dc=cisco,dc=com
   ldap-scope onelevel
   ldap-naming-attribute sAMAccountName
   ldap-login-password altiga
   ldap-login-dn cn=Administrator,cn=Users,dc=nelson,dc=cisco,dc=com
   ldap-attribute-map Our-AD-Map
   5520-1(config)#
   ```
5. Definire un gruppo di tunnel con Autenticazione LDAP o Autorizzazione LDAP. Esempio di autenticazione LDAP. Esegue l'applicazione dei criteri per gli attributi di autenticazione + (autorizzazione) se sono definiti attributi.

   ```
   5520-1(config)# show runn tunnel-group
   remoteAccessLDAPTunnelGroup
   ```

```
tunnel-group RemoteAccessLDAPTunnelGroup general-attributes
authentication-server-group LDAP-AD11
accounting-server-group RadiusACS28
5520-1(config)#
```

Esempio di autorizzazione LDAP. Configurazione utilizzata per i certificati digitali.

```
5520-1(config)# show runn tunnel-group
remoteAccessLDAPTunnelGroup
tunnel-group RemoteAccessLDAPTunnelGroup general-attributes
authentication-server-group none
authorization-server-group LDAP-AD11
accounting-server-group RadiusACS28
authorization-required
authorization-dn-attributes ea
5520-1(config)#
```

6. Definire un criterio di gruppo esterno. Il nome dei criteri di gruppo è il valore del record utente AD-LDAP che rappresenta il gruppo (VPNUserGroup).

```
5520-1(config)# show runn group-policy VPNUserGroup
group-policy VPNUserGroup external server-group LDAP-AD11
5520-1(config)#
```

7. Stabilire il tunnel e verificare che gli attributi siano applicati. In questo caso, il banner e il timeout di sessione vengono applicati dal record VPNuserGroup in Active Directory.

Applicazione di Active Directory dell'opzione "Assegna un indirizzo IP statico" per i tunnel IPsec e SVC

L'attributo AD è msRADIUSFramedIPAddress. L'attributo è configurato in Proprietà utente AD, scheda Chiamate in ingresso, Assegna un indirizzo IP statico.

Di seguito sono riportati i passaggi:

1. Nel server AD, in Proprietà utente, scheda Connessione remota, Assegna un indirizzo IP statico, immettere il valore dell'indirizzo IP da assegnare alla sessione IPSec/SVC (10.20.30.6).
2. Sull'appliance ASA, creare una mappa ldap-attribute-map con questa mappatura:

```
5540-1# show running-config ldap
ldap attribute-map Assign-IP
map-name msRADIUSFramedIPAddress IETF-Radius-Framed-IP-Address
5540-1#
```

3. Sull'appliance ASA, verificare che l'assegnazione dell'indirizzo vpn sia configurata per includere vpn-addr-assign-aaa:

```
5520-1(config)# show runn all vpn-addr-assign
vpn-addr-assign aaa
no vpn-addr-assign dhcp
vpn-addr-assign local
5520-1(config)#
```

4. Stabilire le sessioni di Autorità remota (RA) IPsec/SVC e verificare che il campo Assegnato all'IP (10.20.30.6) mostri vpn-sessiondb remote|svc corretto.

Applicazione da parte di Active Directory di "Autorizzazione di accesso remoto per chiamate in ingresso, Consenti/Nega accesso"

Supporta tutte le sessioni di accesso remoto VPN: IPSec, WebVPN e SVC. Il valore di Consenti accesso è VERO. Il valore di Nega accesso è FALSO. Il nome dell'attributo di Active Directory è msNPAllowDialin.

In questo esempio viene illustrata la creazione di una mappa degli attributi ldap che utilizza i protocolli di tunneling Cisco per creare le condizioni Allow Access (TRUE) e Deny (FALSE). Ad esempio, se si esegue il mapping tra tunnel-protocol=L2TPover IPsec (8), è possibile creare una condizione FALSE se si tenta di imporre l'accesso per WebVPN e IPsec. Si applica anche la logica inversa.

Di seguito sono riportati i passaggi:

1. In Proprietà utente1 server Active Directory, Accesso remoto, scegliere l'opzione appropriata per consentire o negare l'accesso per ogni utente. **Nota**: se si sceglie la terza opzione, Controlla accesso tramite Criteri di accesso remoto, il server AD non restituisce alcun valore, quindi le autorizzazioni applicate sono basate sull'impostazione dei Criteri di gruppo interni dell'ASA/PIX.
2. Sull'appliance ASA, creare una mappa di attributi ldap con questa mappatura:
   ```
   ldap attribute-map LDAP-MAP
   map-name msNPAllowDialin Tunneling-Protocols
   map-value msNPAllowDialin FALSE 8
   map-value msNPAllowDialin TRUE 20
   5540-1#
   ```
   Nota: aggiungere altri attributi alla mappa in base alle esigenze. In questo esempio viene mostrato solo il minimo per controllare questa funzione specifica (Consenti o Nega accesso in base all'impostazione di Accesso remoto).Qual è il significato o l'applicazione di ldap-attribute-map?valore-mappa msNPAllowDialin FALSE 8Nega accesso per un utente1. La condizione del valore FALSE corrisponde al protocollo di tunneling L2TPoverIPsec (valore 8).Consenti accesso per utente2. La condizione del valore TRUE corrisponde al protocollo tunnel WebVPN + IPsec (valore 20).Un utente WebVPN/IPsec, autenticato come utente1 in Active Directory, non riuscirà a causa di una mancata corrispondenza del protocollo del tunnel.Un L2TPoverIPsec, autenticato come utente1 in Active Directory, non riuscirà a causa della regola di negazione.Un utente WebVPN/IPsec, autenticato come utente2 in Active Directory, avrebbe esito positivo (regola Consenti + protocollo tunnel corrispondente).Un L2TPoverIPsec, autenticato come utente2 in Active Directory, non riuscirà a causa di una mancata corrispondenza del protocollo del tunnel.
   Supporto per il protocollo tunnel, come definito nelle RFC 2867 e 2868.

Applicazione da parte di Active Directory dell'appartenenza a "Membro di"/Gruppo per consentire o negare l'accesso

Questo caso è strettamente correlato al caso 5 e fornisce un flusso più logico ed è il metodo consigliato, in quanto stabilisce il controllo dell'appartenenza a gruppi come condizione.

1. Configurare l'utente AD come membro di un gruppo specifico. Utilizzare un nome che lo collochi in cima alla gerarchia dei gruppi (ASA-VPN-Consultants). In AD-LDAP, l'appartenenza ai gruppi è definita dall'attributo di Active Directory memberOf. È importante che il gruppo si trovi all'inizio dell'elenco, in quanto attualmente è possibile applicare le regole solo alla prima stringa group/memberOf. Nella release 7.3, è possibile eseguire il filtraggio e l'imposizione di più gruppi.
2. Sull'appliance ASA, creare una mappa ldap-attribute-map con il mapping minimo:
   ```
   ldap attribute-map LDAP-MAP
   map-name memberOf Tunneling-Protocols
   map-value memberOf cn=ASA-VPN-Consultants,cn=Users,dc=abcd,dc=com 4
   5540-1#
   ```

Nota: aggiungere altri attributi alla mappa in base alle esigenze. In questo esempio viene illustrato solo il minimo per controllare la funzione specifica (Consenti o Nega accesso in base all'appartenenza a un gruppo).Qual è il significato o l'applicazione di ldap-attribute-map?User=joe_consultant, parte di AD, che è membro del gruppo AD ASA-VPN-Consultants può essere autorizzato ad accedere solo se l'utente utilizza IPsec (tunnel-protocol=4=IPSec).User=joe_consultant, parte di AD, può interrompere l'accesso VPN durante qualsiasi altro client di accesso remoto (PPTP/L2TP, L2TP/IPSec, WebVPN/SVC e così via).User=bill_the_hacker NON può essere consentito in poiché l'utente non è membro di Active Directory.

Applicazione da parte di Active Directory delle regole relative all'orario e all'orario di accesso

In questo scenario viene descritto come impostare e applicare le regole relative all'ora del giorno in AD/LDAP.

Di seguito viene riportata la procedura per eseguire questa operazione:

1. Sul server AD/LDAP:Scegliere l'utente.Fate clic con il pulsante destro del mouse su **> Proprietà (Properties)**.Scegliere una scheda da utilizzare per impostare un attributo (ad esempio la scheda Generale).Scegliere un campo o un attributo, ad esempio il campo Office, da utilizzare per applicare l'intervallo di tempo, quindi immettere il nome dell'intervallo di tempo, ad esempio Boston. La configurazione di Office nella GUI è memorizzata nell'attributo physicalDeliveryOfficeName di AD/LDAP.
2. Sull'appliance ASA Creare una tabella di mapping degli attributi LDAP.Mappare l'attributo AD/LDAP "physicalDeliveryOfficeName" all'attributo ASA "Access-Hours".Esempio:
```
B200-54(config-time-range)# show run ldap
ldap attribute-map TimeOfDay
map-name physicalDeliveryOfficeName Access-Hours
```
3. Sull'appliance ASA, associare la mappa degli attributi LDAP alla voce aaa-server:
```
B200-54(config-time-range)# show runn aaa-server microsoft
aaa-server microsoft protocol ldap
aaa-server microsoft host audi-qa.frdevtestad.local
ldap-base-dn dc=frdevtestad,dc=local
ldap-scope subtree
ldap-naming-attribute sAMAccountName
ldap-login-password hello
ldap-login-dn cn=Administrator,cn=Users,dc=frdevtestad,dc=local
ldap-attribute-map TimeOfDay
```
4. Sull'appliance ASA, creare un oggetto dell'intervallo di tempo con il valore name assegnato all'utente (valore di Office al passaggio 1):
```
B200-54(config-time-range)# show runn time-range
!
time-range Boston
periodic weekdays 8:00 to 17:00
!
```
5. Stabilire la sessione di accesso remoto VPN: La sessione può avere esito positivo se è compresa nell'intervallo di tempo.La sessione può avere esito negativo se non rientra nell'intervallo di tempo.

Utilizzare la configurazione ldap-map per mappare un utente in un gruppo di criteri specifico e utilizzare il comando authorization-server-group, in caso di doppia

autenticazione

1. In questo scenario viene utilizzata l'autenticazione doppia. Il primo server di autenticazione utilizzato è RADIUS, mentre il secondo server utilizzato è un server LDAP. Configurare il server LDAP e il server RADIUS. Di seguito è riportato un esempio:

```
ASA5585-S10-K9# show runn aaa-server
aaa-server test-ldap protocol ldap
aaa-server test-ldap (out) host 10.201.246.130
 ldap-base-dn cn=users, dc=htts-sec, dc=com
 ldap-login-password *****
 ldap-login-dn cn=Administrator, cn=Users, dc=htts-sec, dc=com
 server-type microsoft
 ldap-attribute-map Test-Safenet-MAP
aaa-server test-rad protocol radius
aaa-server test-rad (out) host 10.201.249.102
 key *****
```

   Definire la mappa degli attributi LDAP. Di seguito è riportato un esempio:

```
ASA5585-S10-K9# show runn ldap
ldap attribute-map Test-Safenet-MAP
map-name memberOf IETF-Radius-Class
map-value memberOf "CN=DHCP Users,CN=Users,DC=htts-sec,DC=com" Test-Policy-Safenet
```

   Definire il gruppo di tunnel e associare il server RADIUS e LDAP per l'autenticazione. Di seguito è riportato un esempio:

```
ASA5585-S10-K9# show runn tunnel-group
tunnel-group Test_Safenet type remote-access
tunnel-group Test_Safenet general-attributes
address-pool RA_VPN_IP_Pool
authentication-server-group test-rad
 secondary-authentication-server-group test-ldap use-primary-username
default-group-policy NoAccess
tunnel-group Test_Safenet webvpn-attributes
group-alias Test_Safenet enable
```

   Visualizzare i criteri di gruppo utilizzati nella configurazione del gruppo di tunnel:

```
ASA5585-S10-K9# show runn group-policy
group-policy NoAccess internal
group-policy NoAccess attributes
wins-server none
dns-server value 10.34.32.227 10.34.32.237
vpn-simultaneous-logins 0
default-domain none
group-policy Test-Policy-Safenet internal
group-policy Test-Policy-Safenet attributes
dns-server value 10.34.32.227 10.34.32.237
vpn-simultaneous-logins 15
vpn-idle-timeout 30
vpn-tunnel-protocol ikev1 ssl-client ssl-clientless
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Safenet-Group-Policy-SplitAcl
default-domain none
```

   Con questa configurazione, gli utenti AnyConnect a cui è stato eseguito correttamente il mapping con gli attributi LDAP non sono stati inclusi in Criteri di gruppo, Test-Policy-Safenet. Al contrario, sono ancora inclusi nei Criteri di gruppo predefiniti, in questo caso NoAccess.Vedere lo snippet di debug (debug ldap 255) e i syslog a livello informativo:

```
----------------------------------------------------------------------------

memberOf: value = CN=DHCP Users,CN=Users,DC=htts-sec,DC=com

[47]                        mapped to IETF-Radius-Class: value = Test-Policy-Safenet
```

```
[47]                          mapped to LDAP-Class: value = Test-Policy-Safenet

-------------------------------------------------------------------------------

Syslogs :

%ASA-6-113004: AAA user authentication Successful : server = 10.201.246.130 : user =
test123

%ASA-6-113003: AAA group policy for user test123 is set to Test-Policy-Safenet

%ASA-6-113011: AAA retrieved user specific group policy (Test-Policy-Safenet) for user =
test123

%ASA-6-113009: AAA retrieved default group policy (NoAccess) for user = test123

%ASA-6-113013: AAA unable to complete the request Error : reason = Simultaneous logins
exceeded for user : user = test123

%ASA-6-716039: Group <DfltGrpPolicy> User <test123> IP <10.116.122.154> Authentication:
rejected, Session Type: WebVPN.
```

Questi syslog mostrano l'errore poiché all'utente è stato assegnato il criterio di gruppo NoAccess con l'opzione accesso simultaneo impostata su 0 anche se i syslog affermano che è stato recuperato un criterio di gruppo specifico dell'utente.Per assegnare l'utente nel criterio di gruppo in base alla mappa LDAP, è necessario disporre del comando **authorization-server-group test-ldap** (in questo caso, **test-ldap** è il nome del server LDAP). Di seguito è riportato un esempio:

```
ASA5585-S10-K9# show runn tunnel-group
tunnel-group Test_Safenet type remote-access
tunnel-group Test_Safenet general-attributes
address-pool RA_VPN_IP_Pool
authentication-server-group test-rad
 secondary-authentication-server-group test-ldap use-primary-username
authorization-server-group test-ldap
default-group-policy NoAccess
tunnel-group Test_Safenet webvpn-attributes
group-alias Test_Safenet enable
```

2. Ora, se il primo server di autenticazione (RADIUS, in questo esempio) ha inviato gli attributi specifici dell'utente, ad esempio l'attributo IEFT-class, in questo caso l'utente può essere mappato al criterio di gruppo inviato da RADIUS. Pertanto, anche se nel server secondario è configurata una mappa LDAP e gli attributi LDAP dell'utente corrispondono a un criterio di gruppo diverso, è possibile applicare il criterio di gruppo inviato dal primo server di autenticazione. Per fare in modo che l'utente venga inserito in un criterio di gruppo basato sull'attributo di mappa LDAP, è necessario specificare questo comando nel gruppo di tunnel: **authorization-server-group test-ldap**.
3. Se il primo server di autenticazione è SDI o OTP, che non può passare l'attributo specifico dell'utente, l'utente rientra nei criteri di gruppo predefiniti del gruppo di tunnel. In questo caso, NoAccess anche se il mapping LDAP è corretto. In questo caso, sarà inoltre necessario utilizzare il comando **authorization-server-group test-ldap** nel gruppo di tunnel per inserire l'utente nel criterio di gruppo corretto.
4. Se entrambi i server sono gli stessi server RADIUS o LDAP, non è necessario il comando **authorization-server-group** affinché il blocco dei criteri di gruppo funzioni.

Verifica

```
ASA5585-S10-K9# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : test123                  Index        : 2
Assigned IP  : 10.34.63.1             Public IP    : 10.116.122.154
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : 3DES 3DES 3DES         Hashing      : SHA1 SHA1 SHA1
Bytes Tx     : 14042                  Bytes Rx     : 8872
Group Policy : Test-Policy-Safenet    Tunnel Group : Test_Safenet
Login Time   : 10:45:28 UTC Fri Sep 12 2014
Duration     : 0h:01m:12s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

Risoluzione dei problemi

Utilizzare questa sezione per risolvere i problemi relativi alla configurazione.

Debug della transazione LDAP

Questi debug possono essere utilizzati per isolare i problemi relativi alla configurazione DAP:

- debug ldap 255
- debug dap trace
- debug autenticazione aaa

ASA non è in grado di autenticare gli utenti dal server LDAP

Se l'appliance ASA non è in grado di autenticare gli utenti dal server LDAP, di seguito sono riportati alcuni esempi di debug:

```
ldap 255 output:[1555805] Session Start[1555805] New request Session, context
0xcd66c028, reqType = 1[1555805]
Fiber started[1555805] Creating LDAP context with uri=ldaps://172.30.74.70:636
[1555805] Connect to LDAP server:
ldaps://172.30.74.70:636, status = Successful[1555805] supportedLDAPVersion:
value = 3[1555805]
supportedLDAPVersion: value = 2[1555805] Binding as administrator[1555805]
Performing Simple
authentication for sysservices to 172.30.74.70[1555805] Simple authentication
for sysservices returned code (49)
Invalid credentials[1555805] Failed to bind as administrator returned code
(-1) Can't contact LDAP server[1555805]
Fiber exit Tx=222 bytes Rx=605 bytes, status=-2[1555805] Session End
```

Da questi debug, il formato del DN di accesso LDAP non è corretto o la password non è corretta, quindi verificare entrambi per risolvere il problema.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).